## REMARKS

The above amendment and these remarks are responsive to the Office action of 22 Dec 2004 by Examiner David Yiuk Jung.

Claims 1-11 and 15-27 are in the case, none as yet allowed.

### *35 U.S.C. 103*

Claims 1-30 have been rejected under 35 U.S.C. 103(a) over http://www.sans.org/dosstep/index.php ("Sans").

Applicant has amended the independent claims 1, 11, 18, 24, 26, and 27, and canceled claims 12-14 and 28-30.

With respect to claim 1, the Examiner refers to Sans step 2.2 as teaching, inter alia, "issuing a bit mapped challenge" [Office action, page 2].

Applicant traverses this characterization of Sans. Rather, applicant argues, Sans teaches using a ping command to determine if a site is being used as an amplification site. Sans does not teach, as applicant claims, that such is done in response to a login request, nor is a ping command a bit mapped challenge, as applicant claims and as is described in connection with Figure 3 as follows:

> Figure 3 illustrates an example of the challenge/response method. Figure 3 depicts a bit-encoded login challenge question, requiring the user to read a question and answer it. In this example, the login question is "TO ENTER WEBSITE XYZCO, PLEASE CLICK ON THE COW'S TAIL". The significance of bit encoding is that the challenge is not composed of machine readable USASCII or EBCDIC text. Rather, it is a picture of the text, which an ordinary machine cannot understand. A human will have no problem responding correctly, whereas a machine will be unable to do so. By bit-encoding the login challenge, zombies will be foiled from gaining access to the web site and launching attacks from within valid connections. [Specification, page 34, line 20 ff.]

Further with respect to claim 1, the Examiner states:

> "These passages of Sans do not teach 'limited' service in the sense of the claim. Instead, Sans appears to imply that the service should be entirely cut off if the network is being used as a broadcast amplification site. Nevertheless, it was well known in the art to have a 'limited' service for the motivation of having the option to further track the requestor who may not request again if the service is entirely cut off." [Office Action, page 3.]

Claim 1 requires that the imposition of limited service be conditioned upon an invalid response to a bit encoded challenge to a log-in request, and that concept is not taught or suggested by Sans.

Claims 2-10 depend from claim 1, and are similarly distinguished.

However, specifically with respect to claims 3 and 4, applicants traverse the Examiner's suggestion that "such particular features are well known in the art." The claimed "determining from said speed, latency and average queuing network delay a time-out value" relate to concepts which are defined in applicant's specification (See reference to Silverman 1 and Silverman 2, at page 27, line 21) and which applicant asserts are not "well known". Accordingly, the Examiner is respectfully requested to withdraw the rejection of Claims 3 and 4 under 35 U.S.C. 103(a), and allow Claims 3 and 4. However, if the Examiner maintains this rejection, Applicant respectfully requests that the Examiner provide an affidavit attesting to this statement pursuant to 37 CFR 1.104(d)(2).

With respect to claim 11, applicant has amended the claim to specify the network probing test frame transmission and analysis procedure of applicant's invention.

With respect, to claims 11 and 18, the Examiner refers to a "..." service, "a...quality server", and "Test your network...:". Applicant cannot determine from the Examiner's statements or references to what "..." refers, and suspects that these may be clerical or transcription errors. Applicant requests clarification of the Examiner's statements so as to be able to formulate a proper response, if such is required.

With respect to claims 12-17, the Examiner states:

> "...such particular features are well known in the art for the purpose of handling information across computers and of security." [Office Action, page 4.]

Applicants have canceled claims 12-14, and traverse with respect to claims 15-17. As applicant has previously argued, the art cited, and further most surely the art which is purported by the Examiner to be well known in the art but which the Examiner does not cite, do not teach the claimed bit-encoded challenge-response procedure nor the use in a router-based filtering system of signatures derived from discrete speed, streaming speed, and latency of connecting devices failing the bit-encoded challenge-response procedure. Accordingly, the Examiner is respectfully requested to withdraw the rejection of Claims 15-17 under 35 U.S.C. 103(a), and allow Claims 15-17. However, if the Examiner maintains this rejection, Applicant respectfully requests that the Examiner provide an affidavit attesting to this statement pursuant to 37 CFR 1.104(d)(2).

With respect to claim 18, the Examiner cites Sans step 2.2 as purportedly teaching the claimed system, and with respect to claims 18-23, asserts that "such particular features are well known in the art..." (Claims 19-23 depend from claim 18.)

Applicants traverse. Sans step 2.2 does not teach or suggest applicant's claimed low quality server for serving zombie sources and a high quality server for serving legitimate sources. Rather, Sans teaches testing a network to see if it is acting as an amplification site using a "ping" command. There is no teaching of two servers for responding to login requests as applicants claim. The Examiner asserts that it is well known in the art to have a "low" quality server, but cites no such reference. Applicant argues that it is improper to rely on a bare assertion of "well known" (that is, upon personal knowledge) under these circumstances. Accordingly, the Examiner is respectfully requested to withdraw the rejection of Claims 18-23 under 35 U.S.C. 103(a), and allow Claim 18. However, if the Examiner maintains this rejection, Applicant respectfully requests that the Examiner provide an affidavit attesting to this statement pursuant to 37 CFR 1.104(d)(2).

With respect to claims 24-30, the Examiner asserts that "such particular features are well known in the art..."

With respect to claims 24 and 25, applicants traverse. Claim 24 recites creating a template of attack patterns for a plurality of types of network traffic and responsive to the attack patterns, determining if a spike in network traffic is a DDOS attack. Claim 25, which depends from claim 24, adds determining unique speed and latency network attachment characteristics of devices attempting to connect to said network resource. Applicant argues that it is improper to rely on a bare assertion of "well known" (that is, upon personal knowledge) under these circumstances. Accordingly, the Examiner is respectfully requested to withdraw the rejection of Claims 24-25 under 35 U.S.C. 103(a), and allow Claims 24-25. However, if the Examiner maintains this rejection, Applicant respectfully requests that the Examiner provide an affidavit attesting to this statement pursuant to 37 CFR 1.104(d)(2).

With respect to claims 26 and 27, these claims are similar to claim 1. Applicants have amended claims 1 to focus on the bit-mapped challenge in response to a login request. This is a concept which, applicant asserts, is not a feature well known in the art. Applicant argues that it is improper to rely on a bare assertion of "well known" (that is, upon personal knowledge) under these circumstances. Accordingly, the Examiner is respectfully requested to withdraw the rejection of Claims 26-27 under 35 U.S.C. 103(a), and allow Claims 26-27. However, if the Examiner maintains this rejection, Applicant respectfully requests that the Examiner provide an affidavit attesting to this statement pursuant to 37 CFR 1.104(d)(2).

Applicant has canceled claims 28-30.

## SUMMARY AND CONCLUSION

Applicants urge that the above amendments be entered and the case passed to issue with claims 1-11 and 15-27.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

Robert M. Silverman

By

Shelley M Beckstrand

Shelley M Beckstrand
Reg. No. 24,886

Date: 18 Mar 2005

Shelley M Beckstrand, P.C.
Attorney at Law
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: (276) 238-1972
Fax: (276) 238-1545